Number Theory for Computer Scientists 89-256
Question Sheet 2
Due April 5, 2011 // 1 Nisan 5771

Please feel free to e-mail me at `mschein@math.biu.ac.il` with any questions.

(1) Let $a, b \in \mathbb{Z}$, and let $g = (a, b)$. We would like to find a pair $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ satisfying the equation $ax + by = g$. Explain why we may assume, without loss of generality, that $a \geq b \geq 0$. Prove that the following algorithm always terminates in finite time and always outputs a correct answer.
- Step 1: If $a = b$, then output $(x, y) = (1, 0)$ and terminate.
- Step 2: Define $a_0 = a$, $b_0 = b$, $x_0 = 1$, $y_0 = 0$, $r_0 = 0$, $s_0 = 1$. Define $n = 0$.
- Step 3: If $b_n = 0$, then output $(x, y) = (x_n, y_n)$ and terminate.
- Step 4: If $b_n \neq 0$, then use the Euclidean algorithm to write $a_n = qb_n + r$, where $0 \leq r < b_n$. Then define: $a_{n+1} = b_n$, $b_{n+1} = r$, $x_{n+1} = r_n$, $y_{n+1} = s_n$, $r_{n+1} = x_n - qr_n$, and $s_{n+1} = y_n - qs_n$. Increment n by one, and return to Step 3.

Hint: In Step 4, observe that $r = a_n - qb_n = (x_n - qr_n)a + (y_n - qs_n)b$.

(2) Use the algorithm from the previous exercise to find a pair (x, y) such that $19x + 25600y = 1$.

(3) Suppose that Alice uses RSA and publishes the public key $(n, e) = (25957, 19)$. Find the private key d.

(4) If Bob sends Alice the encrypted message $E(m) = 8236$. What was the original message m? Do not use anything more powerful than a typical pocket calculator.

(5) Suppose that Bob is telling Alice what he bought at the shuk. He has written a word in Hebrew as the element $m \in \mathbb{Z}/n\mathbb{Z}$ using the scheme discussed in class (alef = 1, bet = 2, etc.). What did Bob buy?